IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	William M. Brandt	§ §	Art Unit:	2437
Serial No.:	10/729,398	§ §	Confirmation No.:	8841
Filed:	12/05/2003	§ §	Examiner:	Techane Gergiso
For:	METHOD AND SYSTEM FOR PREVENTING IDENTITY THEFT IN ELECTRONIC COMMUNICATIONS	§ § § §	Atty. Dkt. No.:	200901436-1 (HPC.0831US)

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF PURSUANT TO 37 C.F.R § 41.37

Sir:

The final rejection of claims 1-20 is hereby appealed.

I. REAL PARTY IN INTEREST

The real party in interest is the Hewlett-Packard Development Company, LP. The Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 11445 Compaq Center Drive West, Houston, TX 77707, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF THE CLAIMS

Claims 1-20 have been finally rejected and are the subject of this appeal.

IV. STATUS OF AMENDMENTS

No amendment after the final rejection of March 18, 2009 has been submitted. Therefore, all amendments have been entered.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The following provides a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number and to the drawings by reference characters, as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified by a corresponding reference to the specification and drawings where applicable. Note that the citation to passages in the specification and drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element.

Independent claim 1 recites a method for preventing identity theft in electronic communications, comprising the steps of:

> sequencing (Fig. 5:182; Spec., p. 22, ¶ [0054], ln. 1-18) an encryption key transaction from a trusted service for generating for an individual a consumer identifier (Spec., p. 14, ¶ [0035], ln. 1-11; Fig. 3; Spec., p. 15, ¶ [0036], ln. 1-13) by performing the steps of:
>
> issuing (Fig. 5:186) from said trusted service a primary key to the individual (Spec., p. 22, ¶ [0054], ln. 9-10);
>
> issuing (Fig. 5:188) to the individual a unique identifier from said trusted service (Spec., p. 22, ¶ [0054], ln. 10-12); and
>
> permitting (Fig. 5:190) the individual to generate and maintain a consumer-defined sequence through said trusted service (Spec., p. 15, ¶ [0038], ln. 6-11; p. 22, ¶ [0054], ln. 12-13);
>
> allowing the individual to control access (Fig. 5:192) to commercially related use of said consumer identifier by third parties (Spec., p. 19, ¶ [0046], ln. 5-18; p. 22, ¶ [0054], ln. 14-16);
>
> generating (Fig. 5:210) a report for presentation to the individual when at least one of the third parties requests access to information related to the consumer identifier (Spec., p. 20, ¶ [0050], ln. 1-8; p. 23, ¶ [0056], ln. 11-13); and
>
> allowing the individual to control which of the third parties that requested access can access information related to the individual (Spec., p. 20, ¶ [0051], ln. 1-16; p. 22, ¶ [0054], ln. 16-18; p. 25, ¶ [0060], ln. 1-8; p. 26, ¶ [0062], ln. 9-13).

Independent claim 10 recites a system for preventing identity theft in electronic communications, comprising:

> a computer-readable medium (Fig. 1:58) storing one or more instructions (Fig. 2:82; Spec., p. 13, ¶ [0034], ln. 1-10), wherein one or more of the instructions comprise:
>
> instructions for sequencing (Fig. 5:182; Spec., p. 22, ¶ [0054], ln. 1-18) an encryption key transaction from a trusted service for generating for an individual a consumer identifier (Spec., p. 14, ¶ [0035], ln. 1-11; Fig. 3; Spec., p. 15, ¶ [0036], ln. 1-13), said sequencing instructions further comprising:
>
> instructions for issuing (Fig. 5:186) from said trusted service a primary key to the individual (Spec., p. 22, ¶ [0054], ln. 9-10);
>
> instructions for issuing (Fig. 5:188) to the individual a unique identifier from said trusted service (Spec., p. 22, ¶ [0054], ln. 10-12); and
>
> instructions for permitting (Fig. 5:190) the individual to generate and maintain a consumer-defined sequence through said trusted service (Spec., p. 15, ¶ [0038], ln. 6-11; p. 22, ¶ [0054], ln. 12-13); and
>
> instructions for allowing the individual to control access (Fig. 5:192) to commercially related use of said consumer identifier by third parties (Spec., p. 19, ¶ [0046], ln. 5-18; p. 22, ¶ [0054], ln. 14-16);
>
> instructions for generating (Fig. 5:210) a report for presentation to the individual when at least one of the third parties requests access to information related to the consumer identifier (Spec., p. 20, ¶ [0050], ln. 1-8; p. 23, ¶ [0056], ln. 11-13); and
>
> instructions for allowing the individual to control which of the third parties that requested access can access information related to the individual (Spec., p. 20, ¶ [0051], ln. 1-16; p. 22, ¶ [0054], ln. 16-18; p. 25, ¶ [0060], ln. 1-8; p. 26, ¶ [0062], ln. 9-13).

Independent claim 19 recites a computer-readable storage medium (Fig. 1:58) comprising a system for preventing identity theft in electronic communications (Fig. 2:82; Spec., p. 13, ¶ [0034], ln. 1-10), comprising:

> instructions stored on said storage medium for sequencing (Fig. 5:182; Spec., p. 22, ¶ [0054], ln. 1-18) an encryption key transaction from a trusted service for generating for an individual a consumer identifier (Spec., p. 14, ¶ [0035], ln. 1-11; Fig. 3; Spec., p. 15, ¶ [0036], ln. 1-13), said sequencing instructions further comprising:
>
> instructions stored on said storage medium for issuing (Fig. 5:186) from said trusted service a primary key to the individual (Spec., p. 22, ¶ [0054], ln. 9-10);
>
> instructions stored on said storage medium for issuing (Fig. 5:188) to the individual a unique identifier from said trusted service (Spec., p. 22, ¶ [0054], ln. 10-12);
>
> instructions stored on said storage medium for permitting (Fig. 5:190) the individual to generate and maintain a consumer-defined sequence through said trusted service (Spec., p. 15, ¶ [0038], ln. 6-11; p. 22, ¶ [0054], ln. 12-13); and
>
> instructions stored on said storage medium for allowing the individual to control access (Fig. 5:192) to commercially related use of said consumer identifier by third parties (Spec., p. 19, ¶ [0046], ln. 5-18; p. 22, ¶ [0054], ln. 14-16);
>
> instructions for generating (Fig. 5:210) a report for presentation to the individual when at least one of the third parties requests access to information related to the consumer identifier (Spec., p. 20, ¶ [0050], ln. 1-8; p. 23, ¶ [0056], ln. 11-13); and
>
> instructions for allowing the individual to control which of the third parties that requested access can access information related to the individual (Spec., p. 20, ¶ [0051], ln. 1-16; p. 22, ¶ [0054], ln. 16-18; p. 25, ¶ [0060], ln. 1-8; p. 26, ¶ [0062], ln. 9-13).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 1-20 were rejected under 35 U.S.C. § 103(a) as unpatentable over Engberg (U.S. Patent Publication No. 2003/0158960) in view of Nordman (U.S. Patent No. 7,340,438).

VII. ARGUMENT

The claims do not stand or fall together. Instead, Appellant presents separate arguments for various independent and dependent claims. Each of these arguments is separately argued below and presented with separate headings and sub-headings as required by 37 C.F.R. § 41.37(c)(1)(vii).

A. Claims 1-20 were rejected under 35 U.S.C. § 103(a) as unpatentable over Engberg (U.S. Patent Publication No. 2003/0158960) in view of Nordman (U.S. Patent No. 7,340,438).

1. Claims 1, 6-10, 15-19.

Independent claim 1 recites a method for preventing identity theft in electronic communications, comprising, *inter alia*:

- allowing the individual to control access to commercially related use of said consumer identifier by third parties;
- generating a report for presentation to the individual when at least one of the third parties requests access to information related to the consumer identifier; and
- allowing the individual to control which of the third parties that requested access can access information related to the individual.

It is respectfully submitted that the obviousness rejection of claim 1 is erroneous.

To make a determination under 35 U.S.C. § 103, several basic factual inquiries must be performed, including determining the scope and content of the prior art, and ascertaining the differences between the prior art and the claims at issue. Graham v. John Deere Co., 383 U.S. 1, 17, 148 U.S.P.Q. 459 (1965). Moreover, as held by the U.S. Supreme Court, it is important to identify a reason that would have prompted a person of ordinary skill in the art to combine reference teachings in the manner that the claimed invention does. KSR International Co. v. Teleflex, Inc., 127 S. Ct. 1727, 1741, 82 U.S.P.Q.2d 1385 (2007).

The Examiner conceded that Engberg fails to disclose the "generating a report" and "allowing the individual to control which of the third parties" elements of claim 1. 3/18/2009 Office Action at 6. Instead, the Examiner cited Nordman as purportedly disclosing the claimed features missing from Engberg. *Id.*

Contrary to the assertion of the Examiner, Nordman clearly fails to disclose the above combination of elements of claim 1. The Response to Arguments section of the 3/18/2009 Office Action cited column 33, line 63 – column 34, line 10, of Nordman, as purportedly supporting the rejection. This passage of Nordman refers to a Monitor-2 process in which a supervising authority receives a request from **a user** to identify **his/her user information** maintained at a receiving site and/or to provide a status report on such information. Nordman, 33:63-66. Note, however, that the request that is received is from the user to identify **<u>the same</u> user's** own information maintained at a receiving site.

In contrast, according to claim 1, a report is generated for presentation to an individual when at least one of the **third parties** requests access to information related to the consumer identifier. In other words, the request from the user for the user's own information, as taught by Nordman, does not constitute a request from a third party. Column 34 of Nordman continues to describe the supervising authority ensuring that the user requesting access of the user's information is in fact authorized to do so.

Providing status information to a user in response to the request of the same user, as taught in the cited passage in columns 33 and 34 of Nordman, is completely different from generating a report for presentation to the individual when at least one of the third parties requests access to information related to the consumer identifier.

The Examiner also cited other passages of Nordman, including the following: column 3, lines 20-25; column 6, lines 35-48; column 7, lines 16-23; column 8, lines 40-51. The cited column 3 passage of Nordman refers to employing a trusted third party in managing privacy over user data provided from a user device of a user to a receiving party. This is different from generating a report for presentation to the individual when at least one of the third parties requests access to information related to the consumer identifier.

The passage in column 6, lines 35-48, of Nordman refers to a user device configured to control a privacy level of communications with another party, such as a service operator. The cited column 6 passage of Nordman also refers to the user device conducting communications with another party at different privacy levels. This teaching in column 6 has nothing to do with the "generating" element of claim 1.

The passage in column 7, lines 16-23 of Nordman refers to a third negotiation layer that involves anonymous service delivery which can also include anonymous payment possibilities. The column 7 passage also notes that service may be rendered by a service operator without any need to disclose the identity of the user. This has nothing to do with generating a report for presentation to the individual when at least one of the third parties request access to information related to the consumer identifier.

The passage in column 8, lines 40-51, cited by the Office Action refers to an arrangement that provides an approach to allow parties to conduct service interaction at agreed upon anonymity levels and to filter user information, which has nothing to do with generating a report for presentation to the individual when at least one of the third parties requests access to information related to the consumer identifier.

The above constitutes a first point of error made by the Examiner. In addition, the Examiner also erred in arguing that Norman discloses the following element of claim 1: "allowing the individual to control which of their third parties that **requested access** can access information related to the individual." The Response to Arguments section of the Office Action argued that Nordman, in column 34, lines 1-10, teaches such feature of claim 1. 3/18/2009 Office Action at 3. More specifically, the Examiner quoted the following from Nordman:

> Based on such status or the identification of the user information at a site, the user may request the supervising authority to delete, update or change the user information, to change the writes management rules, and so forth.

Note that the status information was provided to the user in response to a request by **the same** user, not a response to a request by third parties. Thus, the passage of Nordman cited by the Examiner cannot possibly disclose or hint at allowing the individual to control which of the **third parties that requested access** can access information related to the individual.

In view of the above points of error made by the Examiner, it is clear that even if Engberg and Nordman were to be hypothetically combined, the hypothetical combination of references would not have disclosed or hinted at all elements of claim 1.

Moreover, in view of the significant differences between the teachings of Engberg and Norman and the subject matter of claim 1, a person of ordinary skill in the art would not have been prompted to combine the teachings of Engberg and Nordman to achieve the claimed subject matter. As specifically noted above, Engberg completely fails to disclose or hint at certain subject matter of claim 1, as conceded by the Examiner. However, Nordman describes a technique or mechanism that is also quite different from the claimed subject matter. More specifically, Nordman relates to a supervising authority providing status information to a user in response to the request of **the same** user, not in response to requests of third parties.

Thus, a person of ordinary skill in the art would not have been prompted to combine the teachings of Engberg and Nordman to achieve the claimed subject matter.

In view of the foregoing, the obviousness rejection of claim 1 over Engberg and Nordman is clearly erroneous.

Independent claims 10 and 19, and their respective dependent claims are also similarly non-obvious over Engberg and Nordman.

Reversal of the final rejection of the above claims is respectfully requested.

2. Claims 2-5, 11-14, 20.

Claims 2, 11 and 20 depend respectively from independent claims 1, 10 and 19, and therefore are allowable for at least the same reasons. Moreover, claim 2 further recites verifying commercially related use of the consumer identifier, which comprises initiating a verification process from a requesting business entity via a secure connection, and comparing the consumer identifier with a predetermined set of database records using the consumer-defined sequence in response to initiating the verification process.

In the rejection of claim 1, the Examiner had equated the virtual identity (VID) described in Engberg as constituting the consumer identifier of claim 1. However, with respect to the "comparing" element of claim 2, the Examiner cited the following passage of Engberg: ¶ [0489]. This passage of Engberg refers to the trusted party (TP) verifying a company signature and confirming this by signing the message and forwarding the message to the related client. The client then verifies the trusted party signature (confirming the company signature), and after checking the agreement, signs the message and returns the signed message to the trusted party.

These tasks are performed in the context of performing an anonymous signature (Engberg, ¶ [0485]). Nowhere in ¶ [0489] of Engberg is there any teaching or hint of comparing the consumer identifier (equated with the Examiner to the virtual identity of Engberg) with a predetermined set of database records using the consumer-defined sequence in response to initiating the verification process.

Moreover, the Examiner had identified a credit card verification process described in ¶¶ [0737] and [0743] of Engberg as constituting the "verification process" of claim 2. Paragraph [0743] of Engberg describes how a client is able to perform payment authentication for a credit card transaction. However, this procedure of Engberg does not appear to be related at all to the anonymous signature procedure in ¶ [0489] of Engberg.

Thus, claim 2 and its dependent claims are further allowable over Engberg and Nordman for the foregoing reasons.

Claims 11 (and its dependent claims) and 20 are also further allowable for similar reasons.

Reversal of the final rejection of the above claims is respectfully requested.

CONCLUSION

In view of the foregoing, reversal of all final rejections and allowance of all pending claims is respectfully requested.

Respectfully submitted,

Date: August 18, 2009

/Dan C. Hu/

Dan C. Hu
Registration No. 40,025
TROP, PRUNER & HU, P.C.
1616 South Voss Road, Suite 750
Houston, TX 77057-2631
Telephone: (713) 468-8880
Facsimile: (713) 468-8883

VIII. APPENDIX OF APPEALED CLAIMS

The claims on appeal are:

1. A method for preventing identity theft in electronic communications, comprising the steps of:

sequencing an encryption key transaction from a trusted service for generating for an individual a consumer identifier by performing the steps of:

issuing from said trusted service a primary key to the individual;

issuing to the individual a unique identifier from said trusted service; and

permitting the individual to generate and maintain a consumer-defined sequence through said trusted service;

allowing the individual to control access to commercially related use of said consumer identifier by third parties;

generating a report for presentation to the individual when at least one of the third parties requests access to information related to the consumer identifier; and

allowing the individual to control which of the third parties that requested access can access information related to the individual.

2. The method of Claim 1, further comprising the steps of verifying commercially related use of said consumer identifier, comprising the steps of:

initiating a verification process from a requesting business entity via a secure connection;

comparing said consumer identifier with a pre-determined set of database records using said consumer-defined sequence in response to initiating said verification process;

presenting a positive or negative confirmation to said requesting business, said business having registered with said trusted service; and

confirming requested information relating to the individual via said secure connection, said requested information having been pre-authorized for presenting to said requesting business entity by the individual.

3. The method of Claim 2, further comprising the step of reporting to the individual the number of times at least one requesting business entity has initiated a verification process.

4. The method of Claim 2, further comprising the step of confirming requested information relating to the individual including the individual's name, address, and photograph.

5. The method of Claim 2, further comprising the step of confirming requested information relating to the individual including the individual's fingerprints.

6. The method of Claim 1, further comprising the steps of storing said consumer identifier on a remote business database system and permitting the individual to modify said consumer identifier through a secure connection to a remote location.

7. The method of Claim 1, further comprising the step of issuing to the individual a unique identifier from said trusted service according to a pre-determined set of business rules associated with a remote business database system.

8. The method of Claim 1, further comprising the step of allowing the individual to control commercial transactions using said consumer identifier.

9. The method of Claim 1, further comprising the step of issuing to the individual a unique identifier from said trusted service, said unique identifier conveying encrypted information relating to the individual's age and locale.

10. A system for preventing identity theft in electronic communications, comprising:

a computer-readable medium storing one or more instructions, wherein one or more of the instructions comprise:

instructions for sequencing an encryption key transaction from a trusted service for generating for an individual a consumer identifier, said sequencing instructions further comprising:

instructions for issuing from said trusted service a primary key to the individual;

instructions for issuing to the individual a unique identifier from said trusted service; and

instructions for permitting the individual to generate and maintain a consumer-defined sequence through said trusted service; and

instructions for allowing the individual to control access to commercially related use of said consumer identifier by third parties;

instructions for generating a report for presentation to the individual when at least one of the third parties requests access to information related to the consumer identifier; and

instructions for allowing the individual to control which of the third parties that requested access can access information related to the individual.

11. The system of Claim 10, wherein one or more of the instructions include instructions for verifying commercially related use of said consumer identifier, comprising:

instructions for initiating a verification process from a requesting business entity via a secure connection;

instructions for comparing said consumer identifier with a pre-determined set of database records using said consumer-defined sequence in response to initiating said verification process;

instructions for presenting a positive or negative confirmation to said requesting business, said business having registered with said trusted service; and

instructions for confirming requested information relating to the individual via said secure connection, said requested information having been pre-authorized for presenting to said requesting business entity by the individual.

12. The system of Claim 11, wherein one or more of the instructions include instructions for reporting to the individual the number of times at least one requesting business entity has initiated a verification process.

13. The system of Claim 11, wherein one or more of the instructions include instructions for confirming requested information relating to the individual including the individual's name, address, and photograph.

14. The system of Claim 11, wherein one or more of the instructions include instructions for confirming requested information relating to the individual including the individual's fingerprints.

15. The system of Claim 10, wherein one or more of the instructions include instructions for storing said consumer identifier on a remote business database system and permitting the individual to modify said consumer identifier through a secure connection to a remote location.

16. The system of Claim 10, wherein one or more of the instructions include instructions for issuing to the individual a unique identifier from said trusted service according to a pre-determined set of business rules associated with a remote business database system.

17. The system of Claim 10, wherein one or more of the instructions include instructions for allowing the individual to control commercial transactions using said consumer identifier.

18. The system of Claim 10, wherein one or more of the instructions include instructions for issuing to the individual a unique identifier from said trusted service, said unique identifier conveying encrypted information relating to the individual's age and locale.

19. A computer-readable storage medium comprising a system for preventing identity theft in electronic communications, comprising:

instructions stored on said storage medium for sequencing an encryption key transaction from a trusted service for generating for an individual a consumer identifier, said sequencing instructions further comprising:

instructions stored on said storage medium for issuing from said trusted service a primary key to the individual;

instructions stored on said storage medium for issuing to the individual a unique identifier from said trusted service;

instructions stored on said storage medium for permitting the individual to generate and maintain a consumer-defined sequence through said trusted service; and

instructions stored on said storage medium for allowing the individual to control access to commercially related use of said consumer identifier by third parties;

instructions for generating a report for presentation to the individual when at least one of the third parties requests access to information related to the consumer identifier; and

instructions for allowing the individual to control which of the third parties that requested access can access information related to the individual.

20. The computer-readable storage medium of Claim 19, further comprising, as a part of said identity theft prevention system, instructions stored on said storage medium for verifying commercially related use of said consumer identifier, said verifying instructions comprising:

instructions stored on said storage medium for initiating a verification process from a requesting business entity via a secure connection;

instructions stored on said storage medium for comparing said consumer identifier with a pre-determined set of database records using said consumer-defined sequence in response to initiating said verification process;

instructions stored on said storage medium for presenting a positive or negative confirmation to said requesting business, said business having registered with said trusted service; and

instructions stored on said storage medium for confirming requested information relating to the individual via said secure connection, said requested information having been preauthorized for presenting to said requesting business entity by the individual.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.